

Compliance



Today's era of regulations— Sarbanes-Oxley Act (SOX), The Health Insurance Portability and Accountability Act (HIPAA), Gramm-Leach-Bliley Act (GLBA)—are driving compliance requirements such as accountability, security, and auditability for daily business operations. Businesses must reexamine their management of paper and electronic documents to avoid fines from regulators and bad publicity concerning security breaches.

This toolkit provides guidance on the important decisions concerning the necessary resources for compliance-ready business.



The ECM Association

1100 Wayne Avenue, Suite 1100
Silver Spring, MD 20910
Tel 301.587.8202 / 800.477.2446

www.aiim.org

Compliance

Table of Contents

Compliance in the Era of Service-Oriented Architecture page 3

The Role of Business Rules Management in Ongoing Compliance Efforts..... page 6

Compliance & Enterprise Content Management page 9

Enterprise Compliance..... page 11

Compliance: A Quick Look..... page 15

Compliance: When Life Gives You Lemons page 17

Compliant Emails..... page 21

Learning the Compliance Lesson..... page 23

The Reality of Regulatory Compliance..... page 25

Building Compliant IT Systems. page 27

Compliance Crazy..... page 31

Compliance and Standards..... page 35

Memo to CIOs: Don't Forget the Business Case for Compliance..... page 38

Compliance: It's Real, It's Relevant, and It's More Than Just Records page 42

Gauging Your Records Audit Readiness..... page 45

A Compliance Blueprint..... page 49

Compliance in the Era of Service-oriented Architecture

As with everything today, you can't escape the need to bring yourself into compliance with whatever regulations pertain to your organization.

If you're involved in enterprise IT, by now you have probably either heard that service-oriented architecture (SOA) is headed your way or you may already be involved in designing and deploying this new IT architectural paradigm. If your role also encompasses Sarbanes Oxley compliance, then you may be confronting a new set of challenges in an already complex situation. This article is intended to highlight some of the compliance issues you might face as your organization embraces SOA.

What is SOA? Briefly, it's an approach to IT architecture that uses open standards, such as XML and Web services, to enable software applications to exchange data and operating instructions using non-proprietary languages and communication protocols. Applications become available as "services," universally accessible, discoverable, and understandable to virtually any other application—whether it is housed in the same server blade or halfway around the world. Though long a goal of the IT industry, the advent of Internet protocols and XML have finally brought about the real thing.

From a pure IT perspective, SOA has great potential to simplify integration between applications and business partners. The technology also enables significant reuse of IT assets because the universal nature of XML allows a developer to write an application one time and expose it to numerous other applications that can access it without the need for proprietary middleware. Major challenges exist, of course, but SOA has gained in credibility and adoption throughout the Fortune 1000.

Compliance and SOA

From the perspective of compliance, though, SOA is a mixed proposition. SOA's promise of simple, rapid-cycling, and cost-effective integration of applications can help with detective controls such as exception monitoring. Improved integration of heterogeneous ERP and general ledger systems can also facilitate the implementation of internal controls. At the same time, there is a definite downside to exposing one's critical business applications to the world so openly.

For instance, take just one of the IT General Controls that an IT manager must document and implement in order to comply with Section 404 of the Sarbanes Oxley Act. The IT Governance Institute's Control Guidance document recommends that, "The SDLC [System Development Life Cycle] methodology ensures that information systems are designed to include application controls

that support complete, accurate, authorized, and valid transaction processing.” (ITGI – IT Control Objectives for Sarbanes Oxley, April 2004)

What is the impact of SOA on this internal control? There are several, but the main one to focus on is how a system that is open for interaction with virtually any other system in the world can ensure “complete, accurate, authorized, and valid transaction processing.” If you have a robust security and governance plan for your SOA, this internal control will not cause you to lose much sleep. However, if you have not considered fully the compliance ramifications of deploying an application based on open standards, you should.

Here’s the catch: SOA involves “machine to machine” or “application to application” interactions. In contrast, most security solutions today emphasize “human to machine” interactions. For example, you might expose a Web service to a portal. Even though the user of the portal is a person, from the viewpoint of the Web service, the “user” is the portal software. Therefore, to meet the SOX 404 IT General Control Objective described above, you would need to make sure your Web service can authorize, authenticate both human and machine users, and provide an audit log of their activities. This might entail mapping an identity repository to the Web service consuming applications, such as the portal.

Compliance, SOA, and DM

In the world of electronic document management, SOA’s security and governance issues raise a number of critical points for compliance. While many corporate documents are extraneous when it comes to compliance, those documents that are used for financial reporting may be bound by the data integrity and auditability requirements mandated by SOX.

According to Sonia Luna, CPA and president of SOX Solutions, “Document management pertaining to SOX is primarily related to supporting the financial impact of the company’s significant account balances. Document retention to critical reports, which supported the findings of a ‘key control’ are necessary to retain for at least seven years. For example, if a company authorized a vendor payment using email, then those emails would have to be retained for seven years.”

Document management processes whose compliance requirements are affected by SOA might also include the storage and access rules for pharmaceutical chemical compounds or petroleum reserves. These kinds of documents bear on financial reporting because their contents may appear as footnotes to explain the valuation of assets on a balance sheet. According to Luna, “The SEC would like some evidence that companies are taking document retention seriously as it affects their SOX internal controls assessments. If the document retention or the integrity of supporting documents were in question (e.g., not reliable) an auditor would have to create a series of tests to conclude that the current SOX testing period as well as past audit periods were in fact valid to substantiate their audit opinion. It’s one more reason why data recovery is becoming a big deal these days.”

To be compliant with this requirement in an SOA setting, then, would require that the security and governance parameters of the SOA affect both preventive and detective controls. It should not be possible for anyone (or any machine) to alter documents used in financial reporting. At least, there should be an audit trail.

The good news is that if you are in a well-run IT organization, you probably already have the basic control development processes in place to transition to SOA without undue compliance-related aggravation. SOA is an incremental technology shift, so it tends to extend existing security and governance policies. Nonetheless, because of its revolutionary and open nature, SOA should prompt you to think through the governance and security aspects of compliance carefully before exposing major systems as part of an SOA.

Hugh Taylor is vice president of marketing for SOA Software (www.soa.com).

The Role of Business Rules Management in Ongoing Compliance Efforts

"Compliance" generally means eliminating the gap between what we should do ("our policy") and what we do ("practice").

"Compliance" generally means eliminating the gap between what we should do ("our policy") and what we do ("practice"). The underlying policies that we manage are varied and come from both external and internal sources, to which they must comply. We have become quite familiar with well publicized external policies that have derived from regulations, including the Sarbanes-Oxley Act of 2002 (SOX). Other externally generated policies based on regulations include Basel II and HIPAA. But not all externally driven policies are regulatory in nature. They can also derive from private sources, such as a contract with outside organizations, which could generate a bank loan. Less discussed, but often equally relevant to any organization, are policies that derive internally. These policies might align to an organizational strategy, such as customer acquisition. They can be driven by an internal operating goal, for example, credit approval as well as the organizations' willingness to take risk. Best practices are another driver, such as vendor selection.

Invariably, compliance or non-compliance occurs most often at a point of decision. These decisions can include key questions such as, Should I approve this loan? Do I have the right to approve this payment or write this check? Is this revenue recognizable? In some cases the compliance issue deals with whether or not the right person made a decision. The issues here are the flow of work and the assurance that within any business process, all critical decisions are being made, and the right people are making them at the right control point. This is typically the domain of business process or workflow technologies. However, at each of these control points, the right identified party makes one or more specific decisions. The decision occurs at a control point where the decision or decisions themselves are the business controls. Business controls are the primary topic of this article.

Compliance to Policy, and the Relationship to Business Rules

At the top of any organization, or in the preamble of any regulation, policy is described as intent. Within a public company, the CEO might declare that "we will be compliant to SOX by the end of our third fiscal quarter." This policy statement then guides the organization, and is broken down organizational level by organizational level until distinct manageable sub-policies come out as manageable and executable entities. The CFO might take the CEO's policy statement and build many lower level policies, such as "we will be conservative in our revenue recognition." Below the CFO, the Controller forms policies that begin to be expressed in ways that can be implemented and executed in practice.

Under the CFO's general policy, the Controller might create a policy around the extension of credit. This policy begins to be described in specific terms, guiding how this decision is formed under the general "conservative revenue" policy. That specificity usually comes out as business decision statements. Statements such as, "If the company has a poor D&B commercial credit score rating of 4 or 5 and a payment history (days outstanding) of greater than 40 days, then deny credit." These are business rules. Wherever there is a business decision, there are business rules that guide that decision. If people are left alone to decide a similar question, they will either be guided by their own judgment or by the rules they use to make this decision. When organized, a business sets policies and explicit rules to guide key decisions.

The key to compliance and these business controls is one of definition (identifying and describing policies and rules reliably), and one of execution (having decisions that are consistent with stated policies and rules).

Business Rules Management Systems and Compliance

As discussed, business process management (BPM) systems help to manage the flow of tasks through well documented processes, assuring work stops at control points (certain tasks within the business flow) where key business controls are executed. All BPM systems manage task flow, but not all manage business rules, or manage business rules correctly. Business rules are the domain of specific tasks where compliance- related decisions are made. There are two key facets of a business rules management system that are critical to an effective compliance implementation.

They are:

- Provide increased control of the compliance decision logic to the experts who understand the domain of that decision.
- Assure that the business rules the domain expert implements are processed correctly.

Increase Business Control over the Decision the Business Owns

One of the key drivers of business rules systems today is the increased need to control and change decision logic (and the business rules associated with those decisions). This is often described as business agility. In order to do this, more control for the definition and change of the business rules must be placed in the hands of the business user (the subject matter experts). Financial models are an exact analog. In 1980, if the business wanted a financial analysis, they would go to M.I.S. (remember those guys) and ask to have a financial analysis built (in COBOL or FORTRAN). The business would write a specification and M.I.S. would write a design and then code and test. In the end, it could be weeks or months before the financial analysis was built. If the specification was interpreted incorrectly and found late in the development or testing process, many parts of the cycle would need to be restarted. Given this cost, only the most critical financial analyses were built. By 1985 early adopters in the business were playing with products such as Lotus 1-2-3, building these same financial models at a fraction of the cost and time. This same paradigm is true with business controls and associated business rules.

Business and technology groups together are spearheading initiatives to separate business decision logic and their associated business rules from the "compiled" application to drive this much needed agility. This is highly relevant to compliance, for two key reasons. First, if compliance automation is forced through a normal technology cycle, only the most critical business controls will

be automated. This is due to the heavier burden of "coding" business rules, versus using a declarative business rules management system. The other reason is change. Often changes in business decision logic need to happen in shorter business cycles- shorter than classic technology cycles. Business rules management systems align to the shorter business implementation and change cycles.

Getting Business Rules Right

It is great to give more control to the business, but with control comes responsibility; the responsibility to get the business logic right that guides key compliance decisions. Whether there is a person making the wrong decision, or a system, if the decision is wrong, then you are not in compliance. There are a number of classic problems with any business logic and business rules in particular. By the way, these same problems often occur in documented policies, even when no automation is attempted. These problems include:

- Ambiguity, or the problem of two rules conflicting with one another
- Incompleteness, or the problem with missing rules
- Unintended logical loop, or the problem with circular logic (often pointed out in spreadsheets)
- Rule overlap, or extra rules that convey the same answer for similar conditions

One approach to finding these problems is to take the business rules formed in the business rules management system and hand them over to a testing organization that uses classic testing tools and techniques to look for problems. This unfortunately fails for two reasons. First, we have forced the agility of the business cycle change into a longer technology testing cycle. Second, classic testing tools break down as the logic of the problems increases in sophistication. For example, a decision that is made up of 10 conditions (what you are basing your decision on, such as the D&B score) and an average of 3 values (the values of each condition, such as the D&B score being 1, 2, 3, 4 or 5) has over 60,000 combinations of data to test. At 12 conditions and 4 average values, the number explodes to over 16 million data sets to test. This combinatorial explosion is intractable for normal testing processes. In looking for a business rules management system, finding a solution that helps to highlight these problems as a part of the rules modeling (as Microsoft Excel points out circular logic within a spreadsheet) is key to assuring that when the business turns over a decision that they have defined through business rules, the decision is correct and reliable.

Conclusion

It is clear that business controls and their associated business rules, whether automated or not, are a core component of any compliance environment. They exist whenever decisions are made. They underlie any control point within a compliance process. It is also clear that when decisions are automated via a business rules management system, great things can happen. Organizational cost can be reduced by delivering more work through any group by automating steps that were previously manual. Organization risk is also affected because decisions that affect compliance are made consistently with much greater support for auditing. Finally, business agility is achieved. Agility has been one of the missing benefits that organizations have waited for since we first started applying technology to business automation.

David Straus (david.straus@corticon.com) is the senior vice president of Worldwide Marketing and Business Development for Corticon Technologies. Corticon's business rules management system (BRMS) delivers business rules modeling, analysis, and automation.

Compliance & Enterprise Content Management

One night stand or long-term relationship?

Around the world, corporate scandals have raised the profile of issues around governance and corporate compliance and led national governments to pass tough governance laws. AIIM research indicates that 29% of users surveyed in the U.S. identified compliance as the main business driver for their information management projects.

Compliance is relevant to everyone. Compliance is not just about legal requirements, but also organizational rules and requests. These could be industry standards or organizational policies and guidelines. Compliance for some is the same as integrity, and this means that you are able to predict and quality assure all your deliverables. Jeffrey Immelt, the chairman and CEO of GE put it this way, "Nothing—not making the numbers, competitiveness, direct orders from a superior—should ever compromise our commitment to integrity." Compliance is therefore seen as a business driver, and not as a cost since it ensures the consistency of a process.

Ensuring Compliance?

Roughly two years ago, AIIM published "*Information Nation*" with Randolph A. Kahn, Esq., and Barclay T. Blair. This book outlines a seven-step approach to information management compliance; providing a business approach to evaluate, design, or improve current information management practices. The Seven Keys are (1) good policies and procedures, (2) executive-level responsibility, (3) proper delegation, (4) program communication & training, (5) auditing and monitoring to measure compliance, (6) effective & consistent enforcement, and (7) continuous improvement.

GE looks at this from a different angle. They see compliance as an ongoing process with three main activities. You need to prevent non-compliance by providing senior management commitment, risk assessment, policies, procedures, and training. You need to detect non-compliance by having compliance reviews, monitoring dashboards, ombudsperson network, and compliance audits. And you need a non-compliance response having an investigation unit, employee discipline, communication, and systems improvement.

The Relationship Between Compliance and ECM

Enterprise content management (ECM) has been promoted as a solution to compliance by many solution providers—is this true? Some vendors are even promoting "SOX in a box" solutions. Other providers of electronic document management, electronic record management, workflow/business process management, email management, scanners, storage, security, etc. are promoting their

products as compliance solutions. GE-defined systems improvement as way to ensure compliance, but the relationship between compliance and ECM depends on what compliance means for your organization. Chris Harris-Jones, research director, Information Management for analyst firm Ovum, defines information management compliance to refer to the following tasks:

- Finding and retrieving information on demand
- Controlling access and confidentiality
- Monitoring and reporting for enforcement
- Comprehensive auditing
- Secure retention and destruction

ECM components and technologies support all of these tasks. For example; the library services in DM helps users find and retrieve information on demand, the security settings control access and confidentiality, audit trail functionality allows you monitor and report usage, and so on. Do you need document, content, or record management? Or do you need workflow or business process management? Both? What about email management?

ECM is not easy, and it has a number of components and technologies. Numerous terms are used interchangeably when discussing the tools that comprise ECM-integrated document management, integrated document and content management, and total content management are a few. Regardless of the precise terminology, ECM capabilities manage traditional content types as well as the new electronic objects throughout the lifecycle of that content. The first of our new online training programs in ECM is now available on our website, and this Fundamentals of ECM Certificate Program is the most convenient and comprehensive way to ensure you have the knowledge necessary to drive your organization forward towards ECM and compliance. Level One of the ECM Certificate Program includes twelve Web-based courses, 60-90 minutes long. Each course is followed by an online assessment covering the course content. Participants may enroll in individual courses or the entire program. Upon completion of all twelve courses and successfully passing each assessment, participants earn the highly regarded AIIM ECM Practitioner Certificate.

Course topics include:

- Introduction to ECM
- Electronic Document Management
- Electronic Records Management/Preservation
- Workflow/Business Process Management
- Web Content Management
- Imaging
- COLD/Enterprise Report Management
- Storage
- Implementing Standards
- Change Management
- Email Management
- ECM-Putting it All Together

Alle Skjekkeland (askjekkeland@aiim.org) is Managing Director of AIIM Europe (www.aiim.org.uk). He has several years of industry experience as manager and consultant for solution providers focused on information and output management.(www.dlm-network.org).

Enterprise Compliance

This article is a further look into how to turn a compliance plan into reality.

Thirty-four voicemail messages. The light on the CIO's phone blinks insistently as she sips the morning's first cup of coffee and contemplates how in the heck the vendor community manages to work so quickly. The internal decision to move forward with an enterprise compliance strategy was just barely finalized in yesterday's staff meeting. Less than 24 hours later she is already being stalked and chances are good that her team is facing the same deluge. With a sigh, she starts to punch through the messages and rolls her eyes at the variety of sales techniques being inflicted via voicemail (indeed, how has she managed to accomplish anything in her career without the eager assistance of all these assertive folks?) Buried within the urgent requests for immediate meetings she discovers that a wide variety of products are being pitched to solve an equally broad interpretation of her "problem." All the more evidence that the dual goals she has established for her project team are on target.

Her first goal is to create a clear vision for how the enterprise compliance solution will change the way people do their jobs. The prospect of a new system is usually greeted with perceived benefits and drawbacks for both users and executive sponsors. Internal opinions are often based in equal parts on historical precedent ("the last IT project was late, over budget, and really missed the boat on my needs"), on myth ("I know about a great shareware solution that does everything!"), and on organizational reality ("sounds great-but who has time to improve?").

The business landscape is littered with technically superior systems that never generated the first dollar of anticipated return because the project team underestimated the effects of cultural confusion, stubbornness, or skepticism. So the CIO is challenging her team to create a clear understanding of needs and a sincere empathy for the real and perceived impact for users and management. In short, they must enthusiastically pursue the "internal sell."

Her second goal addresses technical challenges as highlighted by the hot pursuit of all these vendors. Preliminary research suggests that there are a number of technologies that can drive a compliance strategy, each with different degrees of functionality, maturity, and cost. As with all good technical decisions, hers will be driven by clearly defined business needs. Furthermore, the various options will be evaluated and assessed for compatibility with her existing IT standards. However, past experience has shown her that good technical decisions aren't always predictive of successful projects. For this reason the CIO has defined the concept of total information flow as the anchor for the compliance technical architecture. The goal is to provide a unified view of information across the organization and automate the processes by which information is created, consumed, and retired according to policy. Sorting through technologies, selecting vendors, and implementing a solution will be daunting but for the team's commitment to this goal.

The CIO smiles as she envisions the career advances she might enjoy if she exceeds expectations for this project. Her plan encompasses a strong compliance solution, but so much more—enough pondering for one morning; time to get to work. Before heading out to refill her coffee, she sends a meeting notice to her team. They need to get together right away to work out the details of the plan. The vendors will just have to wait a bit longer before getting to her calendar.

Compliance: Managing Total Information Flow

Effective information management and process improvement has been the Holy Grail for CIOs and their organizations since the birth of the mainframe. In most cases, technology is not the biggest obstacle in their quest. Generations of advancements in systems and software have produced capabilities that were once heralded as radical achievements but are now considered standard fare. Remember WYSIWYG, the precursor to user interfaces that eliminated command line interaction? And how about "the network is the system" (first conceived by Sun's Steve McNealy) when the idea of interconnected systems—much less the Internet—was a dramatic re-thinking of how computers were used? These and many other innovations have indeed revolutionized how technology can be applied in business. However the opportunities to improve information management in the day-to-day happenings of a business remain large.

As technical progress races on, CIOs still wrestle with the same fundamental challenge: get information to the right people, in the right format, at the right time. Compliance is a relative newcomer on the list of business drivers around improved information management. For the enlightened management team, compliance is an opportunity to reshape the flow of information to avoid risk but also to drive improved efficiency in the business. Compliance initiatives can be limited to point solutions around records management or policy automation. However, when viewed across the full lifecycle of information there is opportunity for significant return.

There is a paradigm shift afoot for information management that is readily expressed in both the technology and business issues surrounding compliance. There is complexity to be found in the technology because several market segments can stand alone or in combination to meet requirements. These segments include enterprise software like content management and business process management; as well as vertical solutions that solve specific compliance issues like SOX process auditing or retention policy management. There is also complexity in the business perspective and scope of requirements. The conflicting views of lawyers, records managers, executives, and employees reflect the proverbial blind men touching the elephant.

The paradigm shift addresses the confrontation and resolution of complexity on both sides. The new world requires a marriage between business and technology, and as with all marriages, commitment and compromise is the name of the game. Lawyers and analysts, records managers, and systems administrators must engage productively to define and embrace information management in the name of Compliance.

Make a Good Marriage Between Technologists and Users

Our ambitious CIO has integrated this paradigm into her project plan with her focus on managing the impact of change and creating a unified information flow—but results are not as forthcoming as she'd hoped. A month into the project, the CIO observes a meeting between her analysts and

several key business stakeholders. As the meeting progresses, compromise and commitment are lost in a frenzy of criticism and confrontation. The users are already running low on patience. While sitting in meetings talking about the informational flow the real flow is at a virtual standstill—so what is the point? The IT folks have developed an irrational attachment to several products and are behaving like teenagers with a first crush. IT's premature enthusiasm is a barrier to open interaction with the users so the potential benefits of these products won't see the light of day in this conversation.

The CIO cuts the meeting short and heads over to the Compliance Director's office for some heartfelt venting and commentary about the difficulty of politics, culture, and the burdens of management. Soon, they move on to a productive brainstorming session, revisiting the genesis of the project and arriving at a mutual conclusion: they must re-calibrate their approach to better line up with the project goals.

Several adjustments are needed. First, executive sponsorship must be active and visible to set the example for "the marriage" between technical and business agendas. The CIO and the Director agree to weekly reviews and commit to develop a proactive adoption strategy maintaining the internal sell during the rollout. Adoption activities will include objective metrics—using before and after values—to measure the impact to the business and to continuously drive improvement as the system evolves.

Next, they concede that the scope is overwhelming for the team. "Total informational flow" will be broken down into logical components—in this case, a few departments that are especially motivated by pain or enthusiasm for a new system. The full strategy will be anticipated in all designs so that ultimately an enterprise solution will be delivered, but only as everyone gains experience and confidence. They also agree to reduce timeframes so that successes happen sooner and both technologists and business users gain positive reinforcement from incremental progress.

Organizations that harness diverse opinions and create positive rules of engagement among business and technical contributors will foster an effective project marriage. A natural outcome of this approach is improved communication and a shared understanding of how information is used within and between individual communities. This is highly advantageous in an enterprise compliance strategy. Records managers, who typically handle information at the end of the lifecycle, gain insight "upstream" into the creation and consumption needs of the business. Subject matter experts begin to see the "downstream" effects of how they categorize information as it relates to retention policy. Lawyers can assess information for risk, but also understand how information is a catalyst for opportunity throughout the lifecycle because the organization is more creative, responsive, or effective in making good decisions.

This common definition of the information lifecycle in and of itself promotes a positive environment to achieve compliance goals. It also establishes the foundation of clear requirements from which a relevant technical architecture can be built. Finally, it creates opportunities for automation. If everyone has a consistent operating definition for information (across all types like documents, images, records, digital assets) and for information processes (creating, reviewing, publishing, exchanging, retiring) then automation can be achieved.

Technology Options

But complexity once again lurks around the corner. Yes, it's those pesky vendors again. So many to choose from, all of whom provide "marketing leading" capabilities and dramatic promises for unprecedented results. The good news is that the markets for many of these products are mature and indeed include strong companies with viable, proven products. The bad news is the difficulty in rationalizing the vendor architecture with your target architecture. Do you go for best-of-breed components or a unified platform? Do you connect highly specialized vertical applications with customized integrations or start with a platform and extend it for vertical needs? Enterprise or departmental? Build versus buy? License cost versus total cost of ownership?

Furthermore, compliance solutions can encompass a considerable range of software tools. Imaging, document and content management, certified records management, business process management, workflow, portals, and collaboration to name but a few. Selecting the ideal combination for your environment requires a firm commitment to drive decisions based on needs and to bring an open mind to best leverage vendor capabilities.

It's the end of a very long day and the CIO is chatting up the project with a few members of her team and the lawyer who has given great input for contracts management. He will also be part of the vendor negotiation team. Everyone is upbeat as the project is on track and considered one of the top priorities for the company. Next step: vendor selection. She good-naturedly kicks the team out of her office and flips open her contact file. Time to return a few phone calls and clear the calendar!

Elaine S. Pelletier is co-founder and CEO of Saillant Consulting Group. She works with corporate leadership and industry experts to improve how real people doing real work use technology.

Compliance: A Quick Look

Compliance is on everybody's lips these days, but compliance with what?

Compliance is on everybody's lips these days, but compliance with what? Compliance means different things to different people. For example, if you're an executive at a publicly traded company in the United States, it means compliance with Sarbanes-Oxley, various SEC regulations, and perhaps NASD guidelines.

If you deal with personally identifiable health information, it means compliance with HIPAA requirements. According to the *Merriam-Webster Dictionary of Law*, compliance is defined as an act or process of complying with a demand or recommendation, or observance of official requirements. And it's nothing new. Every organization has certain strictures and requirements it must comply with: tax regulations, documentation of work status, and pay records. Public companies have fallen under Securities and Exchange Commission regulation since 1934. Records management best practices have been evolving for more than 50 years. What is new is the increased visibility of corporate wrongdoing and the zeal with which it is prosecuted; leading to more regulations organizations must be in compliance with.

To answer the question above, the correct answer is "it depends." It depends on the vertical industry the organization is part of as well as industry best practices. It is up to the organization, and its legal and records departments, to determine the various requirements and how best to satisfy them.

The Costs of Compliance

Compliance isn't cheap. A recent AMR Research survey found that companies expect to spend \$5.8 billion dollars this year just for Sarbanes-Oxley compliance initiatives. This equates to up to half a percent of gross revenues-just to come into compliance.

The costs include more than just tools and technologies. Much of the time and money is spent on researching requirements and reviewing processes to determine what is required and how best to comply. As processes change to meet regulatory dictates, employees must be trained on the changes and how to keep the organization in compliance.

Organizations must also take into account Year Two costs, the costs required to sustain compliance initiatives and remain in compliance. In an August 2004 *CIO Magazine* article, John Hagerty, vice president of research at AMR indicated, "People thought that [compliance spending] was going to be here today and gone next year. In fact, compliance spending is going to be growing."

Even where fines and jail time are not involved, an organization that has poor internal controls may be wasting money through duplication of processes and other inefficiencies. As James Damoulakis of Glasshouse Technologies notes in *The Sarbanes-Oxley Compliance Journal*, "Many of the activities associated with Sarbanes-Oxley compliance are things that already should be done as a standard policy in a well-run organization." Organizations that face new compliance requirements should take the opportunity to look for other ways of doing business more efficiently.

Compliance is a Process

Organizations know they have to comply with something, and they may even have a pretty good idea of exactly what they have to comply with. But too few of them believe they know how to comply, and they turn to the vendor community to "just fix it." As the old saw goes, "There ain't no such thing as a free lunch." In the area of regulatory compliance, there ain't no such thing as a magic bullet.

Compliance is more than records management, but good records management is a key piece of most compliance efforts. And compliance requires more than just technology. We can implement software that will make it easier to comply with regulations, and to demonstrate that compliance. We can implement security, and hardware, and encryption, but all of these things taken together do not make an organization compliant.

As more information is gathered, processed, and maintained electronically, it becomes increasingly important to bring IT into the compliance discussion. So how does an organization "do compliance?" The United States Sentencing Commission and the Office of the Inspector General suggest seven elements to a good compliance program:

1. Standards and procedures to prevent and detect criminal conduct
2. Clearly assigned responsibility at all levels (including senior management), adequate resources, and clear lines of program authority
3. Personnel screening related to program goals
4. Training at all levels
5. Auditing, monitoring, and evaluating program effectiveness coupled with non-retaliatory internal reporting systems
6. Incentives and discipline to promote compliance
7. Reasonable steps to respond to and prevent further similar offenses upon detection of a violation

Organizations should start their compliance initiatives by getting records, legal, and IT together and developing a comprehensive approach. Once the foundations—the policies, procedures, and processes—are in place, companies can look to streamline implementation and ongoing compliance with technology.

Jesse Wilkins, CDIA+, LIT, EDP, ICP is a principal with IMERGE Consulting (www.imergeconsult.com), a leading unbiased technology and management consulting firm. A frequent industry speaker, Jesse is involved in both AIIM and ARMA chapter activities and is a member of the 2005 AIIM Conference planning team.

Compliance: When Life Gives You Lemons...

Complying with regulations isn't optional. Make the most of compliance to make your organization more efficient.

Trying to stifle another yawn, the VP of Sales & Marketing makes a halfhearted attempt to appear engaged in today's IT Executive Steering Committee meeting. The painfully detailed technical discussions of the morning session are now being followed by a presentation from the director of Compliance. Fully expecting to reach unprecedented levels of boredom while the director drones on about record keeping in legalese, the VP thinks about solving his latest customer crisis while keeping his eyes focused on the speaker.

The CEO leans forward to indicate to the assembled executives that he considers this important, eliciting a smile from the director as he takes his place to speak. The VP eventually notices that the others are either very engaged in what the director is saying or they are using superior acting techniques to impress the CEO. Not to be outdone, the VP squints (to convey serious thinking about the director's current topic) and picks up the thread of the discussion.

The director is talking about the need to improve the company's ability to recruit and hire quality talent. The VP of Human Resources obviously likes what he's hearing and the CEO is quietly nodding his head. The discussion moves on to financial issues—and the VP braces for the inevitable lecture on records and legislation and potential incarceration of the CEO. Instead, a lively interaction ensues with the CFO around problems in customer care. The director has presented ideas to improve contracts management and invoice processing for major accounts—which was exactly the customer problem the VP was pondering moments ago. He sits up—and startles the VP of Engineering next to him.

The director was allocated thirty minutes on the agenda and has already exceeded that time by fifty minutes. The entire committee is engrossed in an interactive—and unusually animated—discussion around improving efficiency in their departments. The director wraps up with a summary of his vision to improve the organization and flow of information to solve many of the challenges facing the individual department heads. And—with a nod to the CEO—the plan allows the compliance team to meet their goals as well. The CEO smiles, shakes the director's hand and turns to the committee: *"That, Ladies and Gentlemen, is the kind of compliance I like to see."*

Many a senior manager reading this is most likely chuckling. Legal counsel and records managers have likely fallen off their seat, tears streaming, laughing at the absurdity of it all. However, could there be just a few readers, perhaps with a clever gleam in their eye, who share the director's inspiration to make lemonade when the company puckers on regulatory lemons?

The reality is that people at all levels of the organization must participate in compliance if it is to be effective. And if everyone is “doing it” why not leverage this common motivator to drive improvement that goes beyond obligations and into the core of the organization’s collective performance? When viewed in the upside-down context of creating value to the business, compliance has the potential to become compelling.

Conditional Support

Compliance has come out of the back filing room and into daily conversations in the boardroom and at the water cooler. Traditional biases and expectations around the roles and responsibilities for activities like records declaration, retention management, and process validation have sparked a complex debate among the participants (or “victims,” depending upon one’s perspective). Each participating group brings a unique opinion to both the problem and potential solutions.

Employees don’t want the hassle of tracking and classifying information as an extra item on their already lengthy “to do” lists. Often, they struggle just to find what they need, track it down on time, and get it in an accurate, useful format. And why worry about retention policy? Isn’t it easier to save everything off to your personal drive where someone can just ask for it later?

Management has bigger issues to tackle —like delivering results faster, better, and cheaper. Functional managers will tolerate general compliance obligations as necessary overhead in their day-to-day priorities. But they incur the costs of distraction and lost time associated with a drop-everything and- help-the-lawyers fire drill.

Lawyers face the same struggles (and bad jokes) as always. But now, they must convince an organization laser-focused on competition, customers, market share, and profit that the Justice Department and Congressmen Sarbanes and Oxley should also be on their list of things to worry about.

Records managers are enjoying newfound celebrity—people actually know them and invite them to meetings. Yet they suspect the ongoing perception of their role is that of the ever popular “Records Nazi.” A minor consolation is their equally maligned IT counterparts, often clearly living in a parallel universe (at least according to the users) when it comes to automating information and records management.

And last, there is the executive team. They are highly motivated to meet internal and external regulations (especially the ones where jail time is clearly mentioned). But they struggle to fund what can be viewed as a large insurance policy versus money spent to support mainstream business imperatives.

All of the players, with all of their viewpoints, tend to be distracted at some level in understanding and supporting compliance initiatives. The merits of keeping good records and having them available for business or legal reasons are rarely at issue. The challenge for virtually all parties in the compliance equation lies in answering these questions: How much does it cost? What does it do for me?

Two-For-One

In a gathering of interests, much like the above Steering Committee meeting, day-to-day business issues like hiring quality employees and satisfying customers reflect the true business imperatives. And it is the achievement of these imperatives that drive success or threaten failure for the company. So naturally, substantial energy and time is spent to understand the cost and return for solutions that support these goals. In most organizations, healthy internal debate generates an eventual consensus on relative priorities, and then investments are made in the name of efficiency and results.

Not so for compliance. Opportunity cost (what if we don't keep accurate records?) and risk avoidance (shoulda-woulda-coulda avoided that fine/lawsuit/penalty) might be imperatives to legal and records folks, but it doesn't make the "A" list of things keeping most management up at night. And if it does, the cost of compliance within their individual organizations is hard to justify given all the other potential priorities in need of limited funds.

So where in reality-based business does compliance win mindshare over critical business imperatives? How is the VP of Marketing engaged in records management? When does the CEO nod his head to funding for all? The answer, as demonstrated by our savvy compliance director: when better business comes first.

Better business—in the form of effective information management and process improvement—is among the issues regularly contributing to managerial insomnia. There is a distinct link between information management solutions and compliance initiatives. In fact, when information and processes are optimized to drive efficiency, the organization becomes compliance ready almost by default. Sweet dreams are made of a combined investment in better business and compliance.

This is not to say that records management or regulatory activities self-generate and magically fulfill all obligations. However, when information is available to the right people, at the right time, and in the right form as part of a defined business process, then compliance policy can be consistently enforced. It becomes integral to day-to-day activity rather than perceived as disruptive overhead. Nowhere is this potential more apparent than in today's records management systems.

The Brave New World of RM

Historically, RM in commercial organizations has been relegated to an administrative after-thought, performed by clerks toiling in the midst of towering file cabinets, well removed from the throes of meaningful business activity. In highly regulated and government industries, records activities tend to be more visible due to tangible, well understood penalties for non-compliance, but the records process remains largely separate and administrative. The explosion of electronic documents, ubiquity of electronic communication, and acceptance of electronic transactions contradicts the fundamental administrative nature of records. As a result, a new era in records management has rapidly evolved.

RM still fulfills the traditional functions of classifying and retaining information that is vital to the company. But the creation, consumption, and retention of information is now a constant, spontaneous activity due to its electronic format. The number of participants and the amount, size,

and type of information exchanged far exceeds the scope that could ever have been generated by paper-based, manual processes. However, just because a record can be created spontaneously by virtually anyone anywhere, doesn't diminish the importance of the record. Some would argue that it in fact increases both value and risk to the company. Furthermore, the pervasiveness of electronic information raises the level of difficulty in capturing the record at a relevant point, assigning appropriate policy and doing so without interrupting how the record contributes to an active business process.

As our hero the director suggests, putting records management in the context of the business solves the dilemma of "What does compliance do for me?" The answer: it enables an infrastructure to manage information from "womb to tomb" which, in turn, provides improved efficiency to your HR, marketing, engineering, or financial process. It also happens to intelligently make the appropriate (and potentially automated) distinction between "under consumption" and "under retention"—blurring the traditional boundary where it's tossed into the filing room at the end of its active life.

How much does it cost? Opportunity costs and risk avoidance remain near and dear to the lawyer's hearts (or coffers as the case may be). But a records management solution within the context of information management—a.k.a. enterprise content or document management to those in the know—has the added justification of increased efficiency. As our CEO concluded, if the same solution will drive better business while simultaneously keeping him out of jail, then it is a highly leveraged investment indeed.

Back To the Future...

The Committee members scurried off to various afternoon commitments with the satisfaction of time well spent in an unexpectedly productive meeting. The only person to leave the room with a frown was the CIO. She could see that funding wasn't going to be a problem—the justification was strong and the CEO was clearly on board. But how to make the director's vision a reality? Surely, technology will play a significant role, but it wasn't going to be easy. Back in her office, she momentarily stares at her flat screen and then begins to draft her presentation to the committee for next month's meeting. To be continued . . .

Elaine S. Pelletier is co-founder and CEO of Saillant Consulting Group (www.saillant.com). She works with corporate leadership and industry experts to improve how real people doing real work use technology.

Compliant Emails

Managing email at R.W. Smith & Associates is one of the firm's highest priorities. Headquartered in Seattle with 12 offices throughout the U.S., the company is a leading facilitator of trades between securities dealers and dealer banks. As a broker's broker, RWS acts exclusively as an undisclosed agent in the purchase and sale of municipal securities. That puts the firm squarely in the sights of the Securities and Exchange Commission (SEC), which has—in recent years—taken a hard stand against noncompliance. Such Wall Street luminaries as Deutsche Bank Securities, Goldman Sachs, Morgan Stanley, and Salomon Smith Barney have been on the receiving end of significant fines for their failure to retain emails for the SEC-mandated retention periods.

SEC guidelines require licensed brokers to archive emails for a period of at least three years, and to produce email records on request to government auditors. In response, Richard G. Smith, director of IT for RWS, has taken a proactive stance with his firm's policy, preferring to keep everything by default. "It's our reasoning that we retain all emails and filter out those that are disposable later on," he said.

In choosing a solution to manage its email, Smith said the company identified key mandates that provided the guidelines for seeking a solution. The application had to provide support for compliance. It had to have manageable indexing and searching capabilities. And, finally, it had to be affordable and easy to use. The company receives thousands of emails a week, which the software had to index according to pre-determined specifications. These documents, according to Smith, not only had to be secure but also easily accessible by staff and auditors from regulatory authorities.

In seeking a solution, Smith said he looked at a number of products from a variety of vendors. "We were cautious in our approach knowing that the software we chose would not only have to provide security but also have to be cost-efficient, easily integrate with our existing platforms, and be intuitive enough to make it simple for authorized personnel to access.

Based on its guidelines, RWS ultimately chose Alchemy® MailStore, an email archiving solution from Captaris, Inc. "We chose MailStore because it enabled us to quickly meet the strict guidelines outlined in the SEC regulations," said Smith. "There are currently multiple solutions in the marketplace that would have met our compliance objective, but they were too expensive and required high priced 'extras' to work effectively."

MailStore grabs every piece of email from the firm's Microsoft Exchange Server and places it in a secure and compliant repository. Emails are automatically categorized and are searchable by sender, subject, group, and keyword. They can be searched, retrieved, viewed, and their lifecycle carefully managed.

RW Smith takes a tiered approach to archiving the data for compliance. "We have a standard tape library that backs up the data nightly, and once a week we use a totally separate WORM drive from Sony that backups all the MailStore databases. Both tapes are sent to off-site storage. We also have, for immediate drops for auditors or regulators that request certain time periods, a DVD burner on site that allows us to provide the information instantly," Smith said. For additional convenience and searching efficiencies, Smith creates new databases each quarter. "It's much easier to search 70,000 emails rather than have to work through a half a million or so that are captured annually."

Ease of use is critical for R.W. Smith. "When we set up search clients on specific work stations for our chief compliance officer and CEO, I've created very simple "how-to-do" documentation with screen shots and they're immediately up and running.

As an add-on to managing retention policies, Smith has also customized his email retention application to flag any message that violates the company's internal email policies, including messages that could potentially violate sexual harassment policies. "A copy of the offending mail is flagged automatically and is moved to a folder that is searched and viewed by our compliance officer," according to Smith. "Anything that's deemed inappropriate is dealt with accordingly."

Richard G. Smith is the director of IT for RW Smith & Associates, a registered Municipal Securities Broker's Broker, which acts exclusively as an undisclosed agent in the purchase and sale of municipal securities for registered broker/dealers and dealer banks. RW Smith & Associates services the top dealers and dealer banks in the U.S. in addition to some of the largest U.S. securities firms.

Learning the Compliance Lesson

One global enterprise's approach to managing electronic communication in a regulated environment.

Beginning with the Enron scandal in late 2001, the number of requests for enterprises to produce email for review has increased dramatically. Unfortunately, most enterprises have decentralized IT systems and processes, and huge, rapidly growing record stores. These enterprises can spend millions of dollars a year meeting obligations to produce records quickly—and millions more in fines if they fail. Before the wave of corporate scandals began, few companies in any vertical industry actively managed policies covering every type of content in the enterprise, yet the cost of retrieving documents to support litigation was already high.

One large, global bank deployed an active policy management solution to provide both policy enforcement and intelligent surveillance of all electronic communication with minimum disruption to users. Previously, the bank's retention policy was focused solely on backup; the only way it could fulfill requests from regulators was by handing over archive tapes and backup drives, which the regulators had to restore.

Moving beyond the storage, retention, and retrieval problems, the bank discovered another set of problems when they looked at their email system and policies. Personal email distribution lists often mixed groups of users (for example, from the equities division and from research). The bank sometimes inadvertently disclosed information to the wrong parties or prematurely, which violated several regulations, in particular regulations concerning conflicts of interests.

In 2002, the bank decided to reduce the total cost of ownership of its email system, along with the cost of storage. Although compliance requirements were not part of the original project scope, which was about managing email archives and reducing storage costs, the bank recognized that it needed a system to help it meet regulations more quickly and efficiently. In many similar financial institutions, compliance teams review a sample of email messages to see that they don't transgress policy. This bank rejected the approach as incomplete and too resource-intensive.

The bank implemented a system for archiving and searching email, and automating an email management policy. The system would have to segment users and define information-sharing boundaries compatible with regulations. Because no one vendor could meet its needs, the bank assembled best-of-breed components including solutions for:

- Active email archiving (ZANTAZ's Exchange Archive Solution)
- Managing policies in conformance with regulations in the financial industry (Orchestra), and
- Journaling all email messages and writing them to storage (EMC's Centera product).

Many email archiving applications can be configured to monitor the journaling mailboxes of Microsoft Exchange. By doing so, all incoming and outgoing email messages are archived to the determined storage device. The archiving programs retrieve the messages, index the content, create metadata about each message, and store the messages. One type of metadata that can be associated with a message indicates how long the device must retain a message. Given this retention period, the company can prevent anyone from removing the message before the retention period has expired. Used in conjunction with archiving applications, email monitoring programs can help enforce corporate policies. An active policy management (APM) solution applied on the users' desktop can monitor activity and remind users about corporate policies, based on rules maintained by the business users. If the APM solution knows the context in which a message is created, it adds metadata about this context to the rest of the metadata stored.

In addition to significant operational savings, the bank avoids considerable risk and possible associated costs by not transgressing regulatory guidelines. Fewer people are needed to support the infrastructure and manage policies—a savings based on freeing expensive human resources from routine, compliance-related activities.

The bank met its original goal of archiving and searching large volumes of email as mandated by law or required for litigation. The bank has also had or expects the following benefits:

- Highly efficient storage through archiving provides an important benefit, given the massive volumes to manage.
- Messages are stored only once, which saves money and reduces risk.
- The system allows managed deletion, a major goal of a retention policy.
- The bank will reap additional savings when the solution extends to mailbox archiving and .PST migration and consolidation.

As the new regulatory climate demands stricter control of email, instant messaging, Web communications, and other documents, global enterprises must implement policy management and archiving solutions that will meet regulations and retrieval requests.

As the VP of global marketing, Paul Johns, vice president of global marketing for Orchestra, oversees marketing strategies and tactics for Orchestra a company specializing in providing real-time visibility and control of all electronic communications.

The Reality of Regulatory Compliance

While true that compliance is a pain, done properly, it's also an opportunity to get your information management house in order.

Let's face it, regulatory compliance is suffering from a really bad public relations problem! Everyone's grouching and groaning about the difficulties of compliance. Yes, the truth is businesses never want to voluntarily do extra work, especially when it's the government requiring them to do so. The usual response is that regulations cost money, take time, and offer little benefit to the business itself.

Well, the first two parts of that are surely true-it certainly does cost money. In fact recent surveys have shown that a typical corporation will spend \$5 to \$15 million to put Sarbanes-Oxley procedures in place the first year. Then, compliance after that, a quarterly affair, costs another several million in filing, administration, auditing, and new procedure development expenses. It has taken the average company the better part of the year with dedicated resources to manage the ordeal. That's a lot of time, and that's just Sarbanes- Oxley. Not to mention the onslaught of other regulations being forced down the throats of American businesses. No wonder regulatory compliance gets bad press!

Here, good reader, is a little balm for your wounds, some salve for your regulatory blues-a prescription for the practicalities of dealing with the objectionable!

- 1. Put a good face on it.** Create awareness and educate everyone about the benefits.
- 2. Start at the top.** Get executive backing, enlist company executive sponsorship. Become knowledgeable in your company's situation and have them communicate that to management. Seek out visibility with company leaders.
- 3. Get organized.** Most successful companies have taken a project management approach with lead reporting directly to the president/CEO, while 30% outsourced to an accounting or consulting firm. Manage this from a central point with all of the components reporting in to one manager. Gather stakeholders; look at short, medium, and long-range goals; and develop policy.
- 4. Understand the requirements.** Do your homework and understand which regulations apply to your business. Examine what your company is doing now and assess what is needed. Then develop a plan to take you from where you are to where you need to be.
- 5. Build the right team.** Make sure you have representation from the executive committee, the technical components, the lines of businesses, the controller or accounting office, legal, project

management, and your outside auditors. Put the right amount of time, resources, and effort into the oft-overlooked upfront stages-analysis and planning. As with all business initiatives, the right planning results in a far better product, and generally saves a good bit of money and grief too!

6. Use the right resources. As ECM professionals, we know that a great deal of this effort rests on our knowledge of information and content management. If you don't already do so, participate in industry events, seminars, and join associations that are pertinent. Bring that knowledge to bear with respect to storage and retrieval, security, backup and recovery procedures, and access rights management. Make sure the right people are addressing ALL of the needs of this project.

7. Understand the risk. The cost of noncompliance is high-very high- personally high to top executives in many cases. Understand and communicate the financial risks, the threat of incarceration, public shareholder reaction to negative news, negative stock price movement, and industry notoriety. The risk is mitigated by the gain. Understand that too. Compliance with the law should be taken for granted by management, employees, and shareholders alike, but isn't always so. For the protection of the corporation and stockholders these steps must be taken. Further, they improve control effectiveness by identifying weaknesses and correcting them. The truth is companies run better and more profitably once these measures are put in place. Finally, increasing governance structure and practices makes for a much healthier organization. Process information becomes available for use as a decision-making asset and this becomes a foundation for enterprise risk management.

8. Communicate. You can never accomplish all of this in a vacuum. It goes without saying that the business process demands consensus building and broad acceptance and participation. Sending the right message is as important to success as the previous seven elements. Trying to accomplish a formidable change without it is a sure path to failure. Present your concepts and involve others in your cause. Conduct periodic presentations and communications to keep everyone abreast of progress and milestones. Do all of this, and do it well, and your company will have a leg up on the process. And remember, compliance is on the rise. You may as well rise with it!

Steve Kass (stevekass@channelmarketpartners.com), president of ChannelMarketPartners, is a consultant who manages ECM projects and advises companies on strategic alliances and related sales and marketing. He is currently president of the Metro New York Chapter of AIIM.

Building Compliant IT Systems

Compliance is a multi-faceted process. A look at the online clickwrap process illustrates the importance of designing a system with an eye toward compliance from the ground up.

Where an application or online service has legal importance, such as one that uses electronic signatures, the risks of a poorly designed user interface (UI) or system architecture extend far beyond frustrated users and a deluge of help desk requests. In fact, poor design can lead to expensive litigation, severe penalties from government regulators, and negative media coverage that can diminish a company's value and prevent it from achieving its business goals.

Application developers have learned that a properly designed UI improves the success of an application by reducing the user's learning curve, reducing user errors and help desk requests, and promoting efficient and intuitive application use.

However, most developers and designers have not been taught to consider the compliance implications of their UIs and system architectures. As a result, many software applications and online services that in fact have serious legal implications are being developed without their architects having access to the legal information that is needed to protect their organizations from serious legal risks and liability.

An application developer has many masters. He/she must satisfy business requirements and goals, address the strengths and shortcomings of existing technology, and work within timeframes that may not reflect the technological reality. As such, every application is necessarily a compromise. For example, planned features may be excluded because an application launch has to coincide with an important company announcement, or a desired component may be delayed until the next budget cycle.

However, in the development of the ever-increasing number of applications that have legal significance, there is another type of accommodation that must occur. The accommodation that results from the tension between what is most intuitive to the UI and system developer, and what the law requires.

By examining the compliance issues central to the development of a particular type of application—in this case a Web application using a "clickwrap" type of electronic signature, we can begin to understand the range of issues that IT and ECM professionals must address during the design and configuration of IT systems throughout the enterprise.

An Example: A Web Application with Electronic Signatures

One of the “Eight Golden Rules” of user interface design¹ states that developers should allow “frequent users to use shortcuts.”² While this is a fundamental principle for UI design, it is precisely what must be avoided in the case of an online “clickwrap” electronic signature.

A “clickwrap” electronic signature typically refers to an online method for Web users to demonstrate their agreement to some statement or event, such as a privacy policy or an online purchase, by clicking on a button or icon that reads “I Agree,” or something similar.

Although many federal and state laws have cleared the way for this type of electronic signature, these same laws require that, before companies can legally rely upon these signatures, they must establish a process that informs the individual of the significance of the act and captures their consent to use the electronic signature in place of a handwritten signature. There may be several creative ways to design a process that meets these obligations. However, what is clear from federal and state legal requirements as they apply to a clickwrap process is:

- **Significance.** The user should be given every opportunity to understand that by clicking on a button reading “I Agree” or something similar, they are doing something as significant as signing their name on a piece of paper.
- **Replacement.** It should be clearly explained (and evident in the system design) that by clicking “I Agree,” the user is consenting to receive confirmations and other information related to the transaction in electronic form instead of in paper form.
- **Opt-out.** The user should be informed of their right to subsequently withdraw from the electronic delivery process, and of any right they have to receive paper copies of transactional information in addition to the electronic information.
- **Security.** Organizations need to ensure that private customer data and transactional information is treated confidentially, regardless of whether it is in paper or electronic form. As such, the process for assigning an electronic signature (such as an ID and password) to a user for them to subsequently access online accounts and other services must be secure.
- **Technology requirements.** It must be clearly explained what software and hardware users will require to access, print, and locally store their electronic records generated by the process.
- **Forced path.** Lastly, it must not be possible for the user to circumvent or “shortcut” the series of screens, dialogs, and other devices used to impart the required information and capture their actions. Allowing such circumvention would make it impossible to prove that users have received the information that they require in order to provide informed consent to the process. The

¹ These rules were published in Dr. Ben Shneiderman's 1997 book, *Designing the User Interface*, and are also available in many places online.

² The commentary on this “golden rule” states: “Frequent users (or, power users) may be turned off by overly tedious procedures. Allow those users a less tedious procedure for accomplishing a given task.”

operative requirement is to capture convincing proof of what the user saw, when they saw it, and what they agreed to.

Consequently, although the “Golden Rule” regarding user shortcuts is intuitive for the application developer, applying it in the case of the clickwrap process may in fact contravene legal requirements.

Electronic Records of the Clickwrap Process

A fundamental principal of information system design is that content must be separated from its presentation. The benefits of this principle are clear—content unbound from presentation enables the same data to be viewed, processed, and presented in multiple forms, such as in various Web browsers, voice applications, and programs designed for people with disabilities.³ However, it is very important to realize that the “content” of an electronic record required for legal purposes (such as records of an employee’s 401K plan elections made on an intranet application) is much more than mere data. In fact, such “content” must meet requirements for completeness, accuracy, integrity, and reliability.

As such, applying the “content and presentation separation” principle to electronic records can severely minimize their legal effectiveness and thus create unnecessary risk for the company.

Assume, for example, that electronic records from a Web application used for purchasing books online are created in the following way. The data relating to the transaction (i.e., book title, shipping address, etc.) is collected and managed in a database. Then, when the transaction is completed, the data for the transaction is combined into a table that is “printed” as a digital Portable Document Format (“PDF”) file. The PDF file is then emailed to the customer and is deleted from the PDF production system.

In this hypothetical case, the company is relying upon the database as the ultimate source of transaction records for “official” purposes, as they have kept no instance of the actual record as it was delivered to the customer. In other words, although the customer received a record that included content and presentation, the company has only retained a record of the content.

Is the content kept by the company enough for legal purposes? Although there are many ways to create electronic records, federal and state laws, regulations, and guidelines provide many requirements and principles for the creation and retention of electronic records. In addition, the courts have weighed in on these issues. A national online retailer, for example, has faced legal action over allegations that customers received goods they didn’t want even though they had clicked a button on a Web page that was supposed to indicated “NO,” they did not wish to make a purchase.

While the law is still developing on many of these issues, system architects, and those who manage the information generated by such systems, should consider the following questions when making design and configuration decisions:

³ For a thorough overview of the origins of this approach, see Dmitry Kirsanov’s April 1998 column, “The Flesh and Soul of Information,” at www.webreference.com/dlab/9804.

- Record integrity. Can the system be used to prove that transaction information has not been altered in the database after the complete "content and presentation" record was delivered to the customer? What about three years from now?
- Record completeness. If you use a standard electronic form that is populated by the database information, can you prove which form field referred to which database entry?
- For example, does the number "\$2000.12" printed from a database table by itself demonstrate that this number was the total purchase price?
- If not, what other information will be required to prove the meaning of this number, and can that information be managed and delivered in a reliable and complete way over time?
- Can you prove that the standard form template that is populated by the database and delivered in its complete "content and presentation" format to the customer has not changed since the customer received it?
- What about three years from now?
- Record format. Is the record you deliver or make available to the customer capable of being viewed, printed, stored, and accessed over the long term in a complete and accurate form?
- Can you prove over the long term what—exactly—the customer received, including the electronic record's physical appearance, the size of the fonts, and the interrelationship of the various textual and graphical elements of the record?
- Can you prove these things regarding the record that the company retains for legal purposes?

Many of these issues are easily resolved in the paper world. All of the information required to understand a paper receipt or transaction record is typically in one place—printed on the paper itself. A legal authority wishing to see the record can request the paper document and it is apparent "on its face" what the record is and what it represents. In addition, the physical qualities of ink on paper make it difficult to tamper with a paper record without detection. The same cannot be said for most electronic records, which exist in many formats, in many different locations, and in many different parts.

In any case, the creation and management of electronic records for legal purposes is another example of a situation where UI and system developers must pause to consider the fact that the most intuitive, efficient, or "correct" approach to architecture is not necessarily the approach that will meet legal requirements.

Final Thoughts

System developers often find themselves in situations where they are asked to develop software applications and online services that meet a variety of competing business, technological, and legal requirements and goals. The consequences of failing to address business or technological goals in system design are well-understood and taught. However, the consequences of failing to address legal requirements are rarely well-understood and rarely taught. It is the responsibility of technologies, attorneys, and information management professionals to understand and address each other's concerns while working together to create an application that meets business goals and protects the company's interests.

Barclay. T. Blair is director of the Technology Practice at Kahn Consulting, Inc. (www.kahnconsultinginc.com) where he focuses on the business, policy, and management issues of information technology.

Compliance Crazy

Is it just me or has our industry gone mad on compliance?

Every week there are, literally, hundreds of articles written about regulatory compliance. Every ECM, BPM, ERP, CRM, and HR vendor seems to have a compliance solution! With such an abundance of solutions, why is still such a major issue, dominating the media?

Interestingly enough, if you talk to the business executives that are involved with compliance, they have a different perspective: They don't know what the real requirements are or how they should implement them. A lot of the regulations are not yet tested. The requirement for process change is not understood. Many of the new regulations have not yet settled or become law. There are overlapping and sometimes contradicting requirements. The business impact is too expensive. They cannot absorb the speed of change, and so it goes on.

So, on one hand, we have a business environment that does not fully understand the problem, let alone the solution. On the other hand, you have hundreds of vendors with panacea solutions that solve that exact ill-defined problem. Does anyone else see a paradox here?

I do not wish to diminish or trivialize the issues of compliance. I also don't want to imply that the various solutions do not have a role to play in addressing compliance. Panic, confusion, and opportunity, however, have created a very volatile environment, which has the risk of creating bigger problems than the ones it is trying to solve.

Sarbanes-Oxley, HIPAA, Freedom of Information, Basel II, etc. Every industry seems to have its own "flavor" of new compliance pressures, all of which have imposing timescales and threatening repercussions.

Yet, compliance is not new! Anyone working in the pharmaceutical industry through the 90s would know that regulatory compliance is not a problem that you solve-it's a way of life. Whether it is in the research and development part of the industry (with FDA submission regulations and the infamous 21CFR-Part 11) or in the area of manufacturing (with Good Manufacturing Practice guidelines and IT systems validation), every part of their product lifecycle is carefully and continuously monitored, audited, and scrutinized. These companies have dedicated regulatory compliance departments, with regulatory compliance officers sitting on the board and with ongoing interactions with their regulators.

What is even more interesting, perhaps, is that these companies do not use "compliance solutions." The ethos and the function of compliance permeate throughout their core business operation. Any functionality that is specifically required to address regulatory compliance has been

built into the core systems that govern day-to-day operations. In this environment, one achieves regulatory compliance by running standard business activities in a compliant fashion.

Let me take a step back and look at compliance through the eyes of the regulator. What is the main purpose of introducing regulations? To ensure that the business is run consistently, safely, and fairly and with minimal risk to the employees, the customers, and the industry as a whole. In other words, the aim is to create businesses that can pass the three main tests for compliance:

- They operate in a way that they are not breaking the law (become compliant)
- They have in place mechanisms to ensure that they will not break the law in the future (remain compliant) and
- They are able to prove, retrospectively, that they have not broken the law (demonstrate compliance)

So, in that sense, compliance needs to be adopted throughout the operational infrastructure and it relates just as much to changing operational behaviors as it does to information and systems. I mentioned earlier that I believe we currently run a risk of generating more problems through the implementation of individual "compliance solutions" than we are trying to solve. Let me explain why in the context of the three tests described above:

Become compliant:

- Even though certain regulations and legislations dominate the compliance space (Sarbanes-Oxley, Basel II, etc.) the list of regulatory laws that an organization needs to comply with runs into the hundreds. Implementing solutions specifically for the more pressing regulations creates a false sense of security and increases the risk of non-compliance to all the other regulations.
- Each year, this list of laws grows longer and the regulations become more complicated. Any system implemented today needs to be able to address multiple regulations and change its stripes very quickly and efficiently in order to adapt to constant regulation change, without change management becoming a major distraction to daily operations. Competitive businesses cannot afford to wait for systems to catch-up with legislation changes.

Remain compliant:

- This is probably one of the higher risk areas today. There is a very clear distinction, which is often ignored, between **documenting** compliance controls and **executing** compliance controls. A lot of the compliance solutions competing for a share in this market today offer good frameworks for capturing and documenting risks and control processes. Very few solutions, however, extend to the actual implementation of these controls into the operational environment. Testing the controls at regular intervals does not guarantee consistency and repeatability in their implementation. Process controlled, audit trailed, and automated execution of controls, on the other hand, does.
- The other major risk associated with individual "compliance solutions" is in the methods used to populate and update these systems. So long as these systems operate independently from the core transactional systems, any auditing information stored in them is open to errors, omissions, and, potentially, fraud. The only way to

ensure full compliance is if the compliance environment is integrated into, and automatically updated by, the operational systems.

Demonstrate compliance:

- This third test is relatively easy to achieve, assuming that all relevant information has been captured and that organizations are able to quickly locate it; prove its completeness, accuracy, and authenticity; and then report on it. However, the risk with compliance solutions is that a lot of that information has been taken out of its originating context, i.e. the business operational environment. Add to that the complication of having multiple compliance systems to address different regulations, and historical data that have been captured in the context of regulations that have changed over time. Who took what decision when? What was their position at the time and were they authorized to make that decision? What criteria and supporting information was available at the time to base the decision on? What version of the control process was "live" at the time? Imagine the scenario where answering these questions from an auditor or regulator requires aggregating data from multiple core systems and multiple compliance repositories. Apart from the logistical distraction, the discovery costs to support an audit or litigation could make serious dent to the business finances.
- Finally, storing all the relevant information without automating the actual reporting process creates another risk of non-compliance. Having a unified compliance environment, instead of individual solutions, means that workflow tools can be used to control and monitor the regular communications with the regulatory authorities and auditors, the aggregation of disparate data sources and finally all the internal management information around compliance status.
- Compliance cannot be added to an operational environment as an external, additional system. It needs to be woven into the organization's daily life and become an integral part of doing business. In fact, the more transparent the compliance environment becomes to the business, the more likely it is to succeed in satisfying the regulators' original motives.

Integrating compliance **functionality**, such as records management, business process management, information security, auditing, etc. (in other words the "bread and butter" functionality of ECM) into the core operational environment allows that compliance layer to be transparently woven into normal business operations. Compliance then becomes a by-product of doing business, not an additional activity.

Although they may alleviate some of the tactical problems relating to specific regulations, stand-alone compliance solutions, even if based on ECM technologies, have limited shelf life. Until operational systems are transformed into compliant operational systems, compliance will remain an overhead to the core business, bringing its own risks into the mix.

There are too many "compliance solutions" in the market today which range from the trivial to the extremely sophisticated. Even though that market space will obviously consolidate as products start to mature, it is very important not to rush head-on into tactical compliance purchases unless you are fully aware that they are just that: tactical. Consider some of the longer-term issues discussed here and whether a more integrated approach to compliance would actually reduce both costs and risk, giving you a competitive edge in the longer term.

George Parapadakis is FileNet's vertical solutions architect for EMEA and can be reached at gparapadakis@filenet.com. George is also the founder and manager of Document Management Avenue, an international community for document management professionals.

Compliance and Standards

Compliance is a bear of a problem. Standards can help.

Education on compliance is everywhere. A Google search on the word “compliance” yields over 19 million hits—there is an International Compliance Association, a Health Care Compliance Association, countless offices of compliance, plus a multitude of articles and white papers on the topic. Nearly every technology magazine is obsessed with the issue. And weekly emails fill my inbox with offers to help me solve the riddle of Sarbanes-Oxley, Basel II, HIPAA, or the Patriot Act as well as general compliance issues around organizational policy.

AIIM has also provided information on compliance and related issues over the past months. The previous two Industry Watch papers have provided deep insight into the compliance problem in our industry. In “*Back to Basics: The Search for Efficiency and Compliance*”, our research revealed that many solution providers are currently emphasizing compliance and risk reduction themes in their marketing messages in response to the increased awareness brought on by the mismanagement of information and the resulting legislation. The United States is more acutely aware of compliance concerns. In the U.S., 17% of users stated that compliance is a business driver for their ECM technology decisions. In Germany, that number is only 5%; in Brazil, 6%. In a paper produced by ARMA, AIIM, and Cohasset Associates, “*Electronic Records Management Survey: a Call for Action*”, the research data suggests an extremely wide gap between the need to manage electronic records and the reality. It’s a wonder that more companies are not in trouble as a result of poor records management practices—over 41% of respondents stated that their company’s records management programs are only marginal to fair.

Information management compliance as discussed in the book Information Nation: Seven Keys to Information Management Compliance by Randolph Kahn, Esq., and Barclay Blair divides compliance criteria into two broad categories. These include:

- Compliance imposed on an organization from an external source such as a regulatory body, i.e., laws, regulations, and industry standards.
- Compliance that is voluntarily adopted or developed by an organization, i.e., internally developed methods or processes or those developed by associations, voluntary standards, and codes and operating procedures developed by an organization.

While we all understand the intent of compliance from the standpoint of complying to the law associated with acts of Congress, an additional dimension is the role of standards within the issue of compliance. Manufacturers have long understood and appreciated the need to comply with standards. To expand the use of a product, manufacturers knew (and know) that that product must be built based upon industry accepted standards. To differentiate from competitors, manufacturers add more flair or additional functionality to sell their product. Now is the time to take this same

approach in our organizations—adapting basic standards to the unique needs of an organization to ensure compliance with standards.

Why aren't standards used to comply with regulations? There are many reasons. A standard to bring an organization into compliance might not exist. If a standard does exist, it might not be well known. Finally, if the standard exists and is known about, there may be a lack of knowledge of how to implement the standard. While standards can be confusing, these are not insurmountable problems.

Are There Standards Out There?

There are close to 900 standards developers in the United States. It is highly unlikely that each organization only produces one or two standards. If they are like AIIM, a standards developer since 1985, each organization has probably developed one hundred, or more, standards. This is where it gets tough. Out of the thousands of existing standards, how do you decide which ones your organization should use? (If we expand the standards universe to include international standards, the choice explodes to hundreds of thousands of standards to choose from.) You can obtain assistance from AIIM (www.aiim.org/standards) or ANSI, the American National Standards Institute, (www.ansi.org). Through a cooperative arrangement between ANSI, national standards developers, government agencies, and international standards organizations, NSSN: A National Resource for Global Standards (www.nssn.org), provides a listing of all known standards.

The Right Standard Does Not Exist

When the right standard for a particular need doesn't exist, this provides a wonderful opportunity for you to both identify needed standards and to help develop them. AIIM Standards is always looking for new and exciting ideas for standards. If you have an idea, let us hear from you. In order to provide the necessary information for the AIIM Standards Board to review standards project ideas, we ask that you complete a project proposal form that can be found at www.aiim.org/documents/standards/proj-proposal.rtf to summarize your standards project idea. Once the project has been approved, you and anyone else that wants to participate are invited to work on the development of the standard. This may involve several face-to-face meetings as well as conference calls, Web meetings, and lots of email transmissions.

We Don't Know How To Implement Standards.

In 2001, AIIM published *ARP-1, Implementation Guidelines and Standards Associated with Web-based Document Management*. This ARP provided a compendium of standards and technical reports that an organization should consider implementing to ensure that their documents are managed in a standardized manner.

Look to AIIM to provide, in the near future, additional guidance in the form of other AIIM Recommended Practices (ARP) that will help you to better manage your organization's information. These documents will provide step-by-step instructions on how to use the subject technology in easy to understand terminology. They will focus on the appropriate application of processes and best practices to ensure that the technology implementations meet the business needs of the organization.

The first of the AIIM Recommended Practices in this series include:

- **Managing Email as a Corporate Asset.** The focus will be the best practices associated with managing the volumes of email that are received daily and how email policy is essential in an organization. This ARP will identify the elements of the policy, provide implementation guidelines, and, most importantly, guidance on how to promote and educate employees on the policy.
- **Core Elements for Your Information Management Policy.** Developing or re-examining an organization's information management policy is necessary in the days of Sarbanes-Oxley, HIPAA, the Patriot Act, etc. This ARP will guide any organization through the process of drafting a policy to ensure that it contains the required elements to safeguard an organization from legal nightmares.
- **Finding a Needle in a Haystack— Categorizing Your Content.** Identifying the appropriate categories or keywords for documents is key to reducing search time and increasing accuracy of searches. This ARP will discuss methods of categorizing your content for easy location and will provide the best practices for defining and implementing a taxonomy.
- **Managing Instant Messages as Corporate Assets.** The use of instant messaging in organizations is proliferating. Since its introduction, instant messaging has progressed from a nice, social communications tool to a method for conducting business. With the wide use of instant message, organizations are becoming acutely aware of the risk factors and are concerned about protecting corporate information. This ARP will provide best practice guidelines for using instant messaging in organizations to ensure that such use is compliant with information management policies.

In addition to these and other ARPs, AIIM's Fundamentals of ECM Certificate Program, which consists of 10 Web-based courses, in combination with our webinars and Content Management Seminar Series events, will provide the basic knowledge you need to be able to recognize which standards to implement to keep your organization compliant with regulations.

Call To Action

While the intent of this article is not to instill fear, it is a wake-up call that should result in positive actions being taken to protect your organization. Where should you begin? Immerse yourself in the topic. Listen to webinars. Take appropriate Web-based training courses, like AIIM's Fundamentals of ECM certificate program. Read magazine articles on compliance and standards—this magazine included. Attend an AIIM Content Management Seminar Series event when it comes to your neighborhood. Submit standards ideas for future standards that will help your organization, and others, be in compliance. Participate in the development activities. Above all, ask your solution providers for products that are based on standards. Individually, we can make a difference. However, if we pool our resources and knowledge, we can, through the use of standards, ensure compliance with regulations. Now is the time.

Betsy Fanning (bfanning@aiim.org) is AIIM's director, content and standards development. She welcomes any and all comments regarding standards and/or the AIIM standards program.

Memo to CIOs: Don't Forget the Business Case for Compliance

In the "flat-out-whatever-it-takes" Y2K-like rush to meet regulatory compliance deadlines, most organizations never get around to building the business case to justify IT investments necessary to meet regulatory requirements. That is a huge mistake. Since many companies have diverted large parts of their IT budgets to comply with regulations such as the Sarbanes-Oxley Act, there is a tendency to focus too closely on just meeting short-term regulatory requirements, instead of carefully analyzing how compliance initiatives can also fulfill long-term strategic imperatives. Some analysts estimate that the average enterprise now has in excess of 80% of its IT budget tied up in non-discretionary spending (running the existing IT environment), the result of costly legacy systems and the lack of clean, simple, and flexible architectures. This immobility in IT budgets makes it an imperative that new compliance IT projects are not justified with fear, uncertainty, and doubt or regulatory paranoia, but with solid business cases that demonstrate the long-term and strategic benefits of IT investments. Since CIOs are frequently forced to fund compliance projects out of dwindling discretionary IT budgets—sometimes less than 20% of the overall budget—they must get the maximum bang for their buck.

Unlike Y2K, regulatory compliance is here to stay and savvy CIOs are now creating strategic frameworks that measure compliance investments based on the ability to address business objectives, not just short-term deadlines. The best run companies have always used IT for competitive differentiation and to reduce costs through consolidation, increased information accuracy, and optimized business processes. All of these objectives must be integral pillars in any long-term compliance effort involving IT to avoid wasting precious IT budgets.

Data Fragmentation: Deal With It Now Or Pay Later

One of the areas most dramatically impacted by regulatory requirements is what is often called unstructured content—electronic documents, emails, instant messages, paper documents, calendars, Web conference proceedings, voicemail, electronic discussions, Web content, and inter-application transactions are either covered today—or will soon be covered—under one or more regulations.

Unlike the records managed in the database, unstructured content is typically not well organized, not easily found, and controlled only under ad hoc security and access control policies. The departmental heritage of most unstructured content repositories such as email, file servers, and content management systems proliferate risk instead of reducing it because there is no easy way to implement policy across the content.

When content is scattered across hundreds of servers, meeting the common requirements for compliance and legal risk management becomes a dramatically more difficult task. This is largely due to a phenomenon known as "server creep." In response to the rapid proliferation of information, individual departments and workgroups often set up their own servers. While this is a reasonable way to address immediate localized needs, it also means that IT departments lose control of these servers and, therefore, cannot manage them effectively. Rapid, reliable content access is complicated by issues such as not knowing which server the content stored on, what kind of server it is, what version of software it's running, or even that the server and its content exists. In addition, establishment of consistent management policies with regard to such critical activities as folder organization, retention and disposition management, secure access control, action tracking and logging, and even backup planning becomes virtually impossible. Finally, documenting the myriad "locally grown" processes and procedures (or, worse yet, identifying areas where processes and procedures simply don't exist) becomes a similarly challenging task.

Typically, users are also frustrated by excessive server downtime and the difficulty of finding and collaborating on content. Instead, employees will send documents as email attachments and maintain multiple copies of documents on their local desktops—driving up network traffic, increasing storage costs, unnecessarily exhausting employees' email quotas, and creating serious data integrity issues. For many CIOs, it often seems a Herculean task to gain control over the content and knowledge within the company, since it is fragmented across so many repositories.

Build Your Business Case Around Consolidation

Initially, companies have often focused on the regulatory impact on financial and customer IT systems such as ERP and CRM systems. However, financial, employee, and customer records are usually safe and sound in a secure database, while unstructured content is frequently scattered across hundreds of email and file servers - and on desktops and laptop computers. Ironically, unstructured content is often more valuable than structured content - for example, a report analyzing last quarter's results is more valuable than the raw quarterly results that are stored in a database.

This mess of distributed repositories is an easy target for any CIO looking to reduce the amount of the IT budget tied up in non-discretionary spending. The multitude of different departmental systems for content drive higher labor costs, and the need for costly, specialized IT skills, as well as higher software licensing and hardware maintenance costs. The costs of running many distributed servers across an organization can be astronomical when the actual full-time-equivalent (FTE) labor costs are calculated. These business pains offer ammunition for a solid business case for compliance solutions focused on unstructured content control. Architecturally, many CIOs decide that leveraging the database as the foundation for all data and content in an organization is the common sense approach since it leverages existing skills in the organization, consolidates content, and facilitates cross-organizational collaboration by having a single place to share content. After all, it's not accidental that all the important customer and product data ended up there.

Avoid Costly Compliance Silos

Almost everyone can agree that compliance is costly, painful, and guaranteed to be a persistent pain in the neck for CIOs unless the root causes of pain are targeted. For example, according to a recent survey from Foley & Lardner LLP of executives from more than 100 public companies, the

average cost of being public for a company with annual revenue under \$1 billion in the wake of Sarbanes-Oxley has increased \$1.6 million (130%) from the inception of the Act through FY 2003, including an increase of \$736,000 during FY 2003. And Sarbanes-Oxley is just one of many regulations that now impact how IT manages data, and some industries are facing even more regulatory overload. In the United Kingdom, one financial services industry organization is calling for a regulatory moratorium after finding that more than 20 new regulations are due to hit the sector between 2004 and 2006 alone, hurting the competitiveness of banks that are already spending 15% of IT budgets on regulatory compliance activities.

The natural reaction of businesses to the bewildering array of regulatory requirements that must be addressed is to grasp at specific solutions for each requirement. However, this "matrix" of solutions quickly escalates into an unmanageable number of "compliance silos" that create more problems than they solve. What's needed is an environment and architecture that is able to support compliance across all regulations and meet other legal risk management requirements—and to be sufficiently adaptable to deal with the changes in requirements that will inevitably occur in the future. That's why CIOs must focus on adaptability as a key design goal for their compliance architecture—something that can be achieved with open standards interfaces and by having a single data infrastructure that can easily expose the content into different processes and environments.

Target Business Process Gaps

In most organizations, there is also an opportunity to reduce risk by streamlining and automating existing manual processes or by exposing content directly into new processes contextually. Simple steps like integrating two systems using Web services to bridge a gap in an important business process can offer a compelling business case. While the integration may also help apply a control point to a risk revealed during an IT internal controls audit (typically as part of Sarbanes-Oxley section 404 compliance), the long-term benefit of streamlining a manual process with a Web service—or an automated workflow—can help reduce cost in a measurable way as well. Organizations can invest wisely in solutions that allow for the future automation of other manual and approval processes in a repeatable and transparent way—while meeting the regulatory requirements at the same time.

Companies that have already consolidated content can often expose it more easily and intelligently into different business processes. But even without consolidating all content, companies can move incrementally towards content consolidation by targeting high-risk content processes first. For example, regulations may require companies to retain business process documentation created for internal audits for a longer period. Instead of managing this content in a specialized application that requires special care and feeding, companies can manage it in a consolidated low-cost repository, which can later be leveraged for other tactical content control activities, or manage all the content in an entire organization. It's all about laying the foundation today for the future cost savings and process optimizations.

Bottom-line: Go Ahead, Eat Your Cake

In short, CIOs must use compliance as an opportunity to rebalance their IT budgets toward flexibility by focusing on content consolidation, business process optimization, and system adaptability. Reducing the amount of IT budgets that are tied up in non-discretionary spending has

become a barrier that must be overcome for companies looking to use IT for transformative growth and competitive differentiation—not just to comply with the next round of regulatory onslaught. Indeed, the most effective compliance solutions may be those that help reduce risk as well as the amount of IT budgets tied up in non-discretionary spending. Maybe it will turn out that smart companies can have their cake and eat it too—at least when it comes to compliance.

Harald P.F. Collet is principal product manager, Records Management and Compliance Support Products for Oracle Corp. He is responsible for product definition and strategy as well as worldwide go-to-market and customer programs. Additionally, he works closely with Oracle's legal and corporate affairs teams and drives a company-wide regulatory compliance initiative. He is a member of the Association for Information Management Professionals; ARMA, as well as the Sedona Conference Working Group on Electronic Discovery and Production.

Compliance: It's Real, It's Relevant, and It's More Than Just Records

ABOUT THE SURVEY

- This Industry Watch survey was conducted during May and June 2006.
- The survey was administered through an online survey instrument, zoomerang.com.
- A total of 741 end users participated in the survey.
- 582 of the 741 survey participants were from the US or the UK.

Distribution of responses by organization size was as follows:

1 to 100	15.8%
101 to 500	18.5%
501 to 1,000	11.4%
1,001 to 10,000	28.3%
10,001 to 50,000	16.8%
Over 50,000	9.2%

Major vertical industries represented in the survey were:

Government & Public Services – Provincial, State, or Local Level	17.0%
Banking & Finance	9.7%
Utilities, Oil & Gas	9.7%
Manufacturing & Engineering	8.4%
Government & Public Services – Central or Federal Government	7.2%
Insurance	6.5%
Healthcare	5.9%

EXECUTIVE SUMMARY

Key Finding #1

Organizations are still at the beginning stages of determining compliance requirements. To paraphrase Churchill, they are perhaps approaching the “end of the beginning,” but there is a great deal of work still to be done.

- Over 50% of end users describe themselves at a very early stage in considering compliance requirements—either as “we have not yet begun” or “we have begun, but much remains to be done.”

Key Finding #2

End users have a disturbingly narrow view of compliance and what it means for their organization, perhaps because of an over emphasis in the media on such legislation as Sarbanes-Oxley and HIPAA.

- When users view the term “compliance” in their organizations in relation to information management, their recognition is limited primarily to government regulations (84.2%), litigation (62.1%), and paper records management (52.0%).

Key Finding #3

Users have an intuitive feel that “something” is wrong within their organizations relative to managing electronic information, but are having a difficult time mounting a systematic and disciplined approach to meeting the challenge.

- Nearly 2 out of 3 end users (63.3%) have not yet analyzed the risk they face from the mismanagement of electronic information.
- Less than 4 in 10 end users (38.6%) have created a central group focused on managing compliance efforts across the organization.
- 42.6% say their organization “does not yet have a clear approach toward meeting compliance” requirements.

Key Finding #4

When it comes to compliance, Records Managers have a seat on the bus—but they aren’t driving it.

- When it comes to the question of who has the MOST influence in driving compliance decisions, the top decision makers are executive staff (25.1%), Legal (22.4%), and IT (17.7%). Records managers across the implementation continuum play a supporting, not a lead role. Those categorizing themselves as records and document professionals represented 53% of survey responses.

Key Finding #5

Contrary to popular belief, when it comes to compliance, the weakest link is electronic, not paper documentation.

- Nearly 64% of end users believe that there is widespread understanding of what PAPER records are and how they should be retained—vs. 34% when considering ELECTRONIC records.
- 65% of end users believe they have clear policies in place related to PAPER information in the event of litigation—vs. 39% when considering ELECTRONIC information.

John F. Mancini, President, AIIM – The Enterprise Content Management Association, has been President of AIIM since May 1996. Working together with the AIIM Board, staff, and thousands of volunteers around the world, his goal is to help AIIM connect the users and suppliers of enterprise content management (ECM) technologies and services. Prior to joining AIIM, John spent 11 years in various positions at the American Electronics Association in Washington, D.C., most recently as Executive Vice President and Chief Operating Officer. The American Electronics Association is the nation's largest technology trade group. John holds a Bachelor's degree from the College of William and Mary and a Master's degree from Princeton University.

Gauging Your Records Audit Readiness

Why Audit?

In today's world nearly everything produces a record-whether it is a document, email, or transaction. This means that records serve as "institutional memories" for decisions that people make in an organization.

Courts, attorneys, and special interest groups have discovered that records are even more important than witnesses in determining "what did they know and when did they know it." Records can help prove innocence or lack of intent. In order to use them, it is important to make sure that the control, storage, and use of records occur in the "normal course of business" and to demonstrate that the records accurately reflected a particular state in time. But records can also be a liability: high profile court cases with Microsoft, Enron, Martha Stewart, and even Winnie the Pooh have taught people that poor recordkeeping can have serious consequences. New laws like HIPAA and Sarbanes-Oxley increase the penalties by adding criminal jail time. Third party audits of records management policies, procedures, and technology are important to demonstrate that the organization complies with the standards, and industry best practices. Just as outside accounting auditors are required for financial controls and policies, outside records management auditors play an important role in helping an organization improve their compliance and develop "plausible deniability" related to records management.

How Often to Audit?

This decision is based on risk and how fast laws and regulations change. Highly regulated industries like pharmaceutical and financial services should audit every three years while typical corporations and certain not-for-profits generally may audit every five years. Government agencies can typically use a seven-year audit cycle.

1. Records Management

Policies—Plan—Program

All three are necessary for compliance.

Policy Statement. Foundation of any records management strategy. Distinguishes RM as a key part of organizational strategy, sets expectations for employee participation in the normal course of business, and identifies the responsible authority.

Plan. Details rules for creating and capturing records and metadata to include receipt of records from other organizational or outside entities, guidelines for transferring records to other organization units or outside entities, the maintenance of records and associated metadata, disposition (destruction or archival) activities and appropriate documentation of those activities, and third-party (contractor, subcontractor) requirements. Documents all relevant national standards and

legal, regulatory, or contractual documents. Provides for management structures, record inventorying, retention schedules, a corporate filing plan, vital records protection including backup/disaster recovery, records center operations and Information Technology (IT) department obligations, preservation, and records management training, monitoring, and auditing

Program. Includes guidance on the record status of working papers or files and drafts, guidance concerning personal papers, the use and removal of documentary and record materials, a mapping of business activities to various records' lifecycle. Also provide guidance and instructions for documenting policies and decisions, especially those decisions reached orally and for those communicated electronically.

2. Records Inventory

Identifies and quantifies ALL organizational records—paper and electronic. Records are then analyzed for various purposes including records retention, legal protection, and improvement opportunities. In electronic environments, the inventory is also important because each records series must be addressed by specific rules that must be programmed into the system. Use or modify industry standard templates for your internal tracking needs.

3. Vital Records Protection

Identify and protect records necessary for the continuation of operations under emergency conditions. Policy and procedure for these special records must be documented for on and off-site storage as well as backup and disaster recovery for electronic records.

4. File Plan (Filing Plan)

Documents the indexing and classification schemes for arranging, storing, and retrieving records. Usually organized by records series or category. Records series include a description. For each records series, the file plan provides descriptions, recordkeeping requirements, roles, disposition, and associated non-record collections.

5. Regulatory/Legal Compliance

To ensure regulatory and legal compliance, a program should identify:

Laws—Best Practices—Tests/Metrics

6. Retention Schedules

Status timetable before final disposition (destruction or archival), with references to statutes and other legal issues associated records series. Retention should enable an evaluation of records for:

- Administrative purposes include control and review (i.e., external audit), fiscal, and tax purposes.
- Legal purposes may be compliance-based and include statutes of limitation considerations.
- Informational purposes, i.e., research value, are typically determined by business units themselves.

7. Backup/Disaster Recovery

Continuity planning, continuous data protection, and disaster recovery are part of a risk

management strategy. Business continuity planning directly determines how an organization protects and backups its records, metadata, and other information, including frequency and establishment of hot, warm, and/or cold sites.

Backup and disaster recovery plans are somewhat subjective. Rarely will an organization fail a records management audit because of how these plans are produced. Not having a plan for records recovery may put passing a third party audit at risk.

8. Security and Privacy

Policies, procedures, and processes must be developed to ensure protection of all confidential information (requirements will vary depending on record type) when stored, accessed, and transferred. Companies must investigate its record systems and communications to ensure proper:

- Treatment of security designations
- Internal and external access privileges
- Labeling of documents and communications
- Tracking of record creation, access, modifications, deletion, and transfers
- Identification of records under hold orders

Organizations must have a written and communicated policy concerning email and instant messages. If used, both must be addressed in the Records Management Plan. One common way to fail an audit is by not having policies that do not preclude corporate email from being forwarded to personal email accounts. Co-mingling of corporate and personal information is wrong and can have significant implications.

9. Metadata

Metadata management involves information pertaining to records but ancillary to the records themselves. Metadata can serve as retrieval aids, as well as provide for tracking and monitoring of usage, actions, and location (in the case of physical records). Metadata also can provide metrics on business process performance. In the case of ECM or other electronic systems that store records, metadata can also be used instead of legacy applications to store information. In those cases, the ECM system then becomes a line-of-business of application that processes and handles more than just the records themselves.

10. Records Center Operations and IT Obligations

Records Center considerations include managing volume, granularity of accessibility, security provisions at each location, employee screening, transport methods, request and transfer procedures, temperature and humidity control, fire suppression, risks posed by toxic or hazardous materials, and records movement tracking. IT departments generally understand requirements for hot, cold, and warm sites, and protection of electronic information.

11. Preservation

Paper can disintegrate, ink can fade, bits and file formats can be lost, and microfilm can undergo chemical decomposition. For most analog storage (paper, film) preservation is a function of storage conditions and handling. For digital storage, media life and file format must be carefully considered.

12. Disposition Procedures

The destruction or archival of records that no longer must be maintained because their retention

period has lapsed, either immediately (best for risk management) or at regularly scheduled intervals. Disposition policy must address records retained past the retention period due to their business value, and include documentation procedures for recording the rationale behind additional retention.

If archived (whether internally or outsourced), organizations must establish that all operational and administrative needs have been satisfied prior to transfer, and appropriately document records to be transferred. Whether destroying or archiving records, organizations must determine the extent to which it is necessary to retain record metadata.

Disposition Procedure for a Record Series.

Steps must be documented and maintained as records.

1. Assign Authority
2. Document destruction details
3. Suspend destruction
4. Verify retention requirements
5. Update the RM system
6. Destroy copies
7. Meet confidentiality, security, and privacy requirements

13. Records Management Training

Establish a program that covers ALL aspects of the RM program (including management, employees, contractors, etc.) regarding the role that information and records play in serving the organization.

Document and provide regularly. Documentation includes training materials, information about the trainer, attendees, and date and time of attendance.

Combine on-the-job training and formal education. Benefits include reduction in costs and risks due to more efficiencies, standards compliance, and error reduction.

14. Monitoring and Auditing

Organizations must preserve records concerning annual internal monitoring and external auditing activities of the records management program. Whether required by regulatory agencies or as part of a corporate risk management initiative, external auditors will want to review internal monitoring efforts to establish sufficiency, validate completeness, and, possibly, recommend opportunities for improvements and potential efficiencies. Internal monitoring activities should dovetail with corporate training. External auditors will want to review previous audit documentation, findings (including deficiencies noted), and corporate efforts to correct deficiencies.

Written by eVisory. Edited by Bryant Duhon and Janelle Julien, AIIM - The ECM Association

A Compliance Blueprint

Companies must be compliant.

This necessity permeates organizations. Because existing regulations are revised and new ones created continuously, compliance is a moving target—a company is never finished with a compliance initiative. To most effectively cope with the ever-evolving need to comply with multiple regulations simultaneously, companies should develop a culture of compliance. This culture is focused on the implementation of policies, procedures, practices, and audits as part of everyday business operations. A framework is needed.

This framework is not just a technology framework. The framework involves a shift in thinking of compliance as an ongoing process, not a one-time project. And, while technology is not a fix for compliance, compliance efforts are stymied by a lack of automation, in many organizations, for moving documents and records through a compliance process. Information technology will be part of the framework. A key piece of the framework is turning compliance into how a company operates and not just another project to stay out of trouble. Doing so will, while keeping companies in line with pertinent regulations, create improved control over their business records and content, an additional benefit.

Building a compliance framework allows regulations to be systematically integrated into the daily work of the organization. New regulations won't stop coming. A company cannot effectively remain in compliance by responding to each regulation separately. A compliance framework creates a repeatable process—using established technology, governance, training, etc.—that can be tweaked for existing and/or new regulations as they change. This minimizes the impact on company operations.

By establishing a compliance framework, complying with regulations—government, industry, or company—specific—becomes embedded in how a company does business.

HOW COMPLIANT ARE YOU?

Laggards

- Deal with compliance manually
- No processes identified for being sufficiently compliant
- Try to manage email by limiting size of mailboxes
- Absence of policies and procedures related to records
- No prioritization and no conflict resolution guidelines in place
- Lack of good taxonomy and master classification plan
- No comprehensive records schedule
- No corporate-wide privacy, security, and retention governance body

Majority

- Point solutions for compliance automation
- Strong policies and procedures identified
- Processes that need tracking and monitoring well defined
- Email management identified as a problem; no clear solution
- Strong master classification plan and robust taxonomy
- No effective strategy for search
- No overall framework for compliance ?? Inadequate business unit and central records schedule in place ?? Chief compliance officer in place

Leaders

- Look at compliance as strategic initiative
- Have a compliance architecture or technical framework
- Strong balance of technology and process excellence
- Have clear rules for records management policy
- Have automated prioritization and role conflict resolution
- Strong master classification plan and robust taxonomy
- Actively managed enterprise-wide records policy and up-to-date retention schedule
- Chief compliance officer and active governance committee selling and enforcing policies

Regulations

Sarbanes-Oxley receives the most attention, but compliance is not limited to topical Federal regulations. All companies have multiple levels of regulations that they must adhere to: national (multiple national regulations if an international company), state and local, industry-specific, and internal governance procedures. Because these regulations change even as new ones are created, companies need an overall framework to address all of these levels, not a SOX plan and/or a Patriot Act plan, etc.

Cost of Discovery

The lack of a compliance plan adds tremendously to the cost of discovery-not to mention that courts are being less forgiving on companies that claim they cannot come up with the proper information. In almost every case, systems and maintenance costs will provide solid ROI through keeping discovery costs low by making relevant business records readily available

COMPLIANCE ACTION ITEMS**Get serious about compliance**

- Realize that compliance is an ongoing reality; don't just comply in a reactive mode

Balance and prioritize your requirements

- Weigh compliance vs. other risk reduction requirements
- Weigh risk reduction vs. other business requirements (operational efficiency, IT consolidation, etc.)

Conduct an internal audit for all relevant regulations

- Identify gaps in your compliance processes and assets
- Evaluate organizational readiness to change

- Prioritize your activities and initiatives

Establish ongoing processes to evaluate and ensure compliance

- With top down leadership
- With education and training
- With ongoing monitoring and evaluation

Evaluate how your current IT environment might be used to support compliance, and what additional tools may be required

- ECM, BPM, RM, integration, etc.

Start with a smaller-scale effort

- With clearly defined objectives, and a limited universe of processes, documents, sources, formats

Build on a successful content management or email archiving deployment

- Adding compliance capabilities to an existing solution is less of a jolt

Address the many enabling conditions for success, including

- Cleanup and taxonomy
- Documented and executed policies and practices
- The need to address both physical and electronic content
- Clear top-level leadership, backed by delegated accountability
- Commitment to training and communication

Analyze how well candidate solutions fit your organization's preferences and risk profile

- Do you favor best-of-breed solutions involving multiple vendors, or integrated offerings that bring multiple components together?
- Do you have the expertise in-house to implement and maintain the solution?
- Does the vendor's solution align with your existing IT environment and standards? With your future IT vision?

Technology Enables Compliance

Technology is a key enabler of a compliance initiative. While one should be wary of vendor claims to "compliance solutions," the following shows compliance-enabling tools and where they fall on a continuum in relation to what can directly be applied to compliance issues and what cannot.

NOT COMPLIANCE:

Network services, document management, business intelligence, storage management, operating systems, and content integration.

COMPLIANCE:

Imaging, classification, BPM, email management, records management, compliance reporting, litigation support, rules engines, and taxonomy.

© AIIM - The ECM Association (2006)
 Written by Bryant Duhon, AIIM - The ECM Association; Jeetu Patel and Rick Tucker Doculabs